

# National Infrastructure Advisory Council (NIAC)

## The Insider Threat to Critical Infrastructures

**Thomas Noonan**  
Former General Manager  
IBM Internet Security Systems

**Edmund Archuleta**  
President and CEO  
El Paso Water Utilities

## Overview

- ▣ Objective
- ▣ Scope
- ▣ Overview: Effort to Date
- ▣ Recommendations Overview
- ▣ Stakeholder Roles and Outcomes
  - President
  - Congress
  - DHS and Federal Agencies
  - Sector Partners
  - CIKR Operators
  - The Public
- ▣ Summary
- ▣ Questions

## Scope

---

- The Study addressed the deliverables assigned in the January 16 letter from Secretary Chertoff in two phases:
  - Phase I (January 2007 – October 2007)
    - Define the “insider threat” physical and cyber, including potential consequences, economic or otherwise
    - Analyze the dynamics and scope of the insider threat including critical infrastructure vulnerabilities
    - Analyze the potential impact of globalization on the critical infrastructure marketplace and insider issues
    - Identify/define the obstacles to addressing the insider threat
  - Phase II (October 2007 – March 2008)
    - Identify issues, potential problems, and consequences associated with screening employees
    - Identify legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
    - Identify and make policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation)

3

## Objective

---

- First Phase focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization
- The Second Phase of the study focused on addressing legal, procedural, and policy barriers to private sector infrastructure operator employee screening efforts
- The study has produced recommendations for stakeholders that when adopted will enable CIKR operators to manage the risk from the insider threat

4

## The Study's Effort to Date

---

- ▣ Held 4 workshop meetings to discuss key issues and develop the recommendations
- ▣ Held 45 conference call discussions
- ▣ Met with 28 Subject Matter Experts

5

## Recommendations Overview

---

- ▣ Policy recommendations for near term solutions:
  - Establish insider threat resources
  - Communicate threat awareness
  - Support improved employee screening
- ▣ Path forward for highly complex issues:
  - Globalization risks for CIKR operators
  - Technology solutions and tools
  - Understanding the relationship between criminal history and employment risk

6

## Stakeholders: The President

---

- ▣ Accept and implement the Report and its recommendations
- ▣ Establish the recommended Executive Outreach and Awareness program within the Executive Office of the President

7

## Stakeholders: Congress

---

- ▣ Read the report to gain understanding of recommended policies
- ▣ Provide criminal history records access to CIKR owners and operators for employee screening, per the 2006 Attorney General's report
- ▣ Implement low-cost, high-return solutions for improving CIKR security against insider threats
  - Insider Threat Outreach and Awareness
  - Insider Threat Clearinghouse Support function
- ▣ Federal agencies have good ideas on insider threats – need to cross pollinate and communicate these ideas

8

## Stakeholders: DHS and Federal Agencies

---

- ❑ Implement near-term recommendations
  - Share information on insider threat risks
  - Establish insider threat clearinghouse resource
- ❑ Establish, plan, and coordinate follow-on work and Research
  - Globalization research
  - Technology solutions research
  - Supply chain vulnerability solutions
- ❑ Establish ongoing dialog to communicate the Report's message to the relevant audiences

9

## Stakeholders: Sector Partners

---

- ❑ Implement recommendation for Sector-specific insider threat information sharing mechanisms (ISACs and SCCs)
- ❑ Coordinate with report-recommended government resources
- ❑ Educate and Communicate to Sector CIKR owners and operators:
  - Insider threat awareness and risk
  - The findings and resources in the Report

10

## Stakeholders: CIKR Operators

---

- ▣ Become informed on the insider threat to critical infrastructures
- ▣ Apply insider threat risk discovery approaches to develop an optimal insider threat program
- ▣ Use best practices frameworks to begin tailoring an insider threat mitigation program
- ▣ Work with established information sharing/clearinghouse Sector organizations on insider threat information sharing

11

## Stakeholders: Value for the Public

---

- ▣ Provide a new path toward improved security and more reliable critical infrastructure services
  - Vital to economic stability, public health, confidence in institutions, and general public welfare.
- ▣ Employee screening approach balances public's concerns with security needs

12

## Summary

---

- ▣ The NIAC was able to define the insider threat to critical infrastructures and outline the growing effect of globalization
- ▣ Reviewed the legal and policy issues surrounding the insider threat and employee screening
  - Recommend adopting provisions of the 2006 Attorney General's Report
- ▣ Recommendations provide public and private sector CIKR partners the means to better manage the insider threat
- ▣ The NIAC found individuals and organizations with expertise on aspects of the insider threat
  - The recommendations will help to distribute this knowledge and these best practices
- ▣ More research needs to be done on globalization issues and technology solutions

13

---

## Questions?

14